A report on the Implementation of web-based appointment and scheduling management information system for Queens Medical Centre

Launching into Cyber Security

PG Cert Cyber Security

Dr Samuel Danso

University of Essex

30 January 2022

Background

Queens medical centre is an NHS clinic serving the local community in the catchment area of Lincoln City Council's Birchwood Ward. The current ward's population is 9000 residents. The current medical staff consists of three part time female doctors, two full time male doctors, two nurse practitioners, two nurses, and three healthcare assistants. Non-medical staff include practice managers, nine receptionists, and two secretaries. The practice offers a wide range of services including chronic and ongoing medical conditions, ante-natal clinic, vaccinations, minor surgery, and physiotherapy. See Appendix A for a real-life example.

Presently, the majority medical appointments and consultations with specialists are scheduled over the telephone through the receptionists. This allows for verbal communication between receptionist and patient allowing for flexibility in complex situations; for example, a patient who is pregnant and has diabetes requires appointments with ante-natal and diabetes clinics.

However, there are certain disadvantages to this system. The current ward population is increasing due to net migration and high-birth rates resulting in the clinic receiving an increasing high volume of calls for appointments. This added workload reduces the outcome for patients due to limited availability of receptionists, appointments slots, and specialists. (Zhao et al., 2017). This is further explored by Akinode and Lekan who note traditional appointment systems are inefficient as they include human errors and multiple and long-winded telephone calls (2007).

ASMIS

According to Zhao et al, there two main types of web-based appointment and scheduling management information systems (ASMIS): software as a service (SaaS) and proprietary built (2017). SaaS ASMIS is cloud-based service built and maintained by third party information technology providers such as Microsoft's Power Apps and System Bookings' online booking system (see Appendix B). This cloud-based architecture can be fully integrated into the clinic's website and management systems.

Potential advantages

The implementation of ASMIS has several key benefits for the Queens clinic and patients. ASMIS reduces the workload as the volume of calls for appointments is expected to decrease allowing receptionists to focus on other duties. No-show and waiting time rates are reduced as patients can easily access the ASMIS portal, peruse the calendar to make, change, cancel appointments at any or place; they are not restricted by conventional working hours or human gatekeepers (Zhao et al, 2017). Other advantages include a reduction in waiting room congestion, overall costs; an increase in patient accessibility, and patient satisfaction (Akinode and Lekan, 2007).

Potential disadvantages

Although technology and portable Internet-connected devices are prevalent in modern society, it is assumed that certain demographic groups are unable to use web-based appointment systems due to medical, physical, financial, and age-related issues. Other factors include lack of awareness, human contact preference, and a digital skills gap (Zhao et al, 2017).

There are also disadvantages for Queens medical clinic. Transitioning from traditional appointment system to web-based system will incur short-term costs and investment in implementing the new centralised system, staff training, and a new administrative structure, which can impact service delivery for the patients.

Cyber and information security is a major concern. Public facing or front-end access portals are prone to malicious attacks including website spoofing, social engineering, and brute force attacks. In 2017, Emory Healthcare appointment system was breached resulting in patient's appointment database being deleted with the attacker demanding a ransom to return the data (Landi, 2017).

Design Approach

From a Cyber security perspective, the Confidentiality, Integrity, Availability (CIA) triad is defining principle for keeping systems and information secure (e.g., Personally Identifiable Information (PII), financial assets, databases, and professional reputation). These principles align with regulatory and legal compliance with the Data Protection Act 2018 and the General Data Protection Regulation 2016 which aim to define how organisations use and protect citizen's data.

Under the Security Principle of the Data Protection Act, organisations must prevent unauthorised access, processing and destruction of personal data (GOV.UK, 2018). Article 32 of GPDR states entities must ensure ongoing confidentiality, integrity, and availability of processing systems and services (PrivacyTrust, 2018).

There are various approaches to understanding perceived threats that can compromise these objectives. According to Rumbaugh, Booch and Jacobson, attack trees and Unified Modelling Language (UML) diagrams have been used in IT industry for over thirty years ‘to capture and precisely state requirements and domain knowledge so that all stakeholders may understand and agree…’ (2010: 13). Another widely used concept is the STRIDE method. Microsoft engineers, Kohnfelder and Garg developed the six-letter mnemonic to better understand security threats to their software design process in the 1990s (Khan et al., 2017).

Attack tree analysis

Attack and defence tree analysis is a security modelling technique originating in the intelligence industry in the 1980s. It draws on the concept of analysing threats and vulnerabilities from the threat actor’s point of view. According to Löhner and Niedermayer, attack and defence tree models have two main advantages: they offer different levels of information within the model, and they are mathematically well defined. Conversely, they are restricted to static processes and in defence priorities. (2018). Figure 1 and 2 shows examples of simple attack and defence trees.

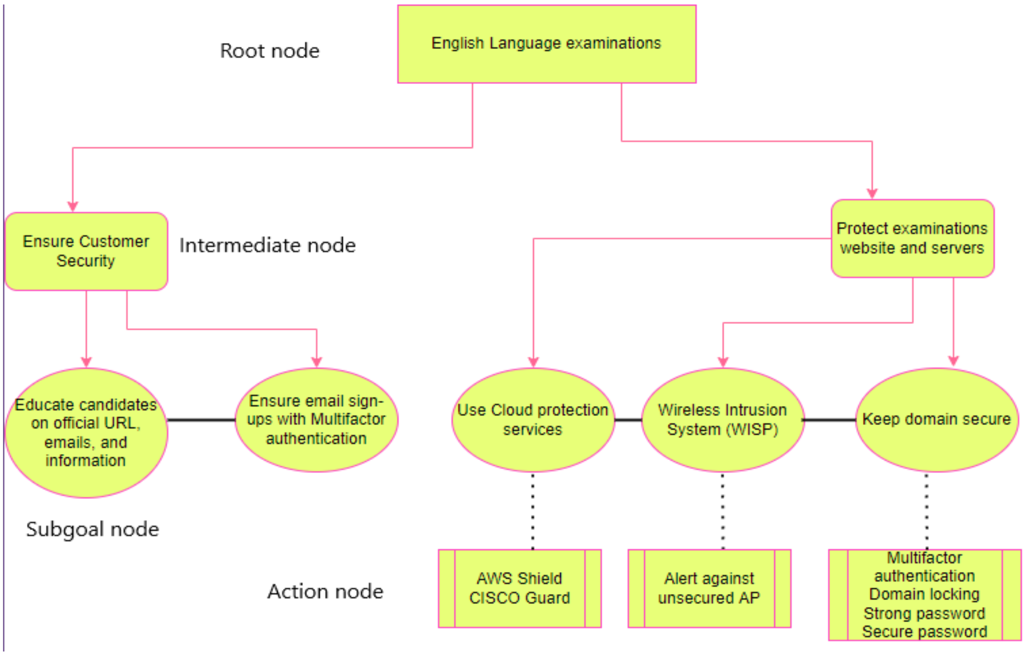

Root node
English Language examinations
Ensure Customer Security
Intermediate node
Protect examinations website and servers
Educate candidates on official URL, emails, and information
Ensure email sign-ups with Multifactor authentication
Use Cloud protection services
Wireless Intrusion System (WISP)
Keep domain secure
Subgoal node
Action node
AWS Shield CISCO Guard
Alert against unsecured AP
Multifactor authentication Domain locking Strong password Secure password

Figure 1. Defence tree

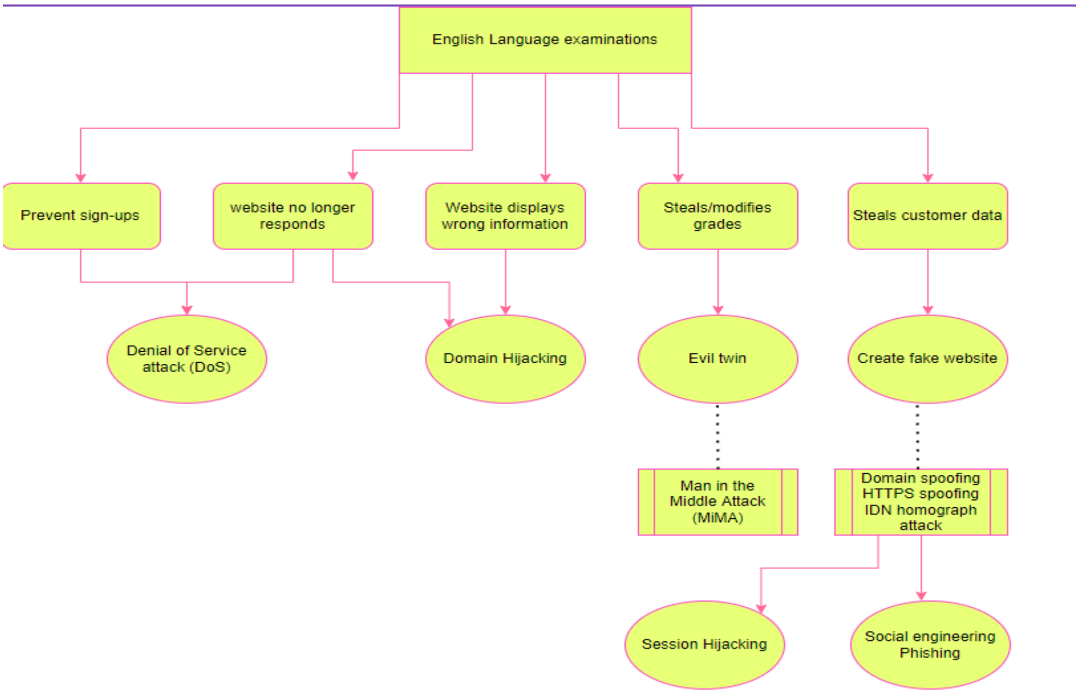

English Language examinations
Prevent sign-ups
website no longer responds
Website displays wrong information
Steals/modifies grades
Steals customer data
Denial of Service attack (DoS)
Domain Hijacking
Evil twin
Create fake website
Man in the Middle Attack (MiMA)
Domain spoofing HTTPS spoofing IDN homograph attack
Session Hijacking
Social engineering Phishing

Figure 2. Attack tree

Attack and defence trees are designed to be hierarchical in nature. The parent or root node is always at the top and represents the attacker's main objective. This is followed by the intermediate node which demonstrates strategies the attacker might use, and the subgoal node highlights how the do accomplish goals and objectives. The final node gives information on the specific tools needed by the attacker. The defence tree will also follow the same process detailing mitigating features. (Ingoldsby, 2021).

STRIDE

Khan et al' demonstrated the significance of the STRIDE method in their research on STRIDE-based Threat modelling for cyber physical systems. They acknowledge its advantages as a comprehensive lightweight systematic approach for analysing security threats. Despite this, they note that current literature and research still does not have a standard methodology for applying STRIDE (2017). Table 1 outlines the STRIDE model.

Action	Outcome
Spoofing	Imitation of legitimate process, system, and user
Tampering	Editing or modification of legitimate information
Repudiation	Deniability of a system executed action
Information disclosure	Unauthorised access or data breach of confidential information
Denial of Service	Service disruption for legitimate users
Elevation of privilege	Attaining higher level access through restricted authority

Table 1. STRIDE Method (Khan et al, 2017)

Unified Modelling Language

The unified Modelling Language (UML) is a combination of earlier object-orientated languages and is widely used and respected in the software industry for object-orientated modelling (Priestley, 2004). UML uses many different models and diagrams to suite the various components of a software design which can be clearly understood by all stakeholders such as coders, analysts, and testers. Table 2 highlights common UML classifications.

Area	View	Diagrams	Concepts
Structural	Static	Class diagram	Class, association, dependency
	Use case view	Use case diagram	Use case, actor, association
Dynamic	State machine view	State-chart diagram	State, event, action
	Interaction view	Sequence	Interaction, object, activation

Table 2 UML classifications (Rumbaugh, Booch and Ivar Jacobson, 2010)

It is beyond the scope of this report to explain full details of each UML diagram; however, the examples below show each UML diagram’s function (See Figures 3,4,5).

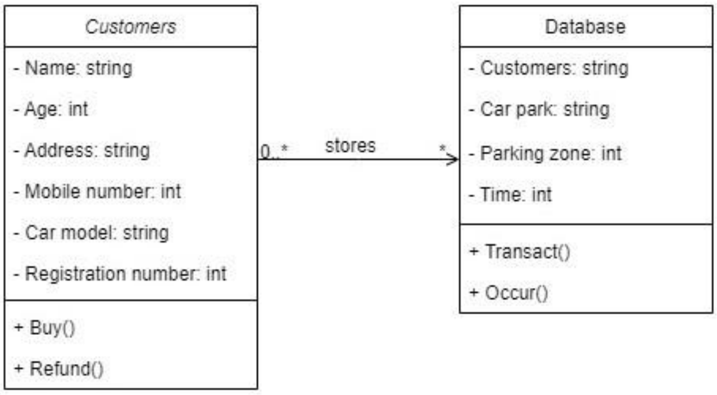


Figure 3. Class diagram of a customer-database parking app domain

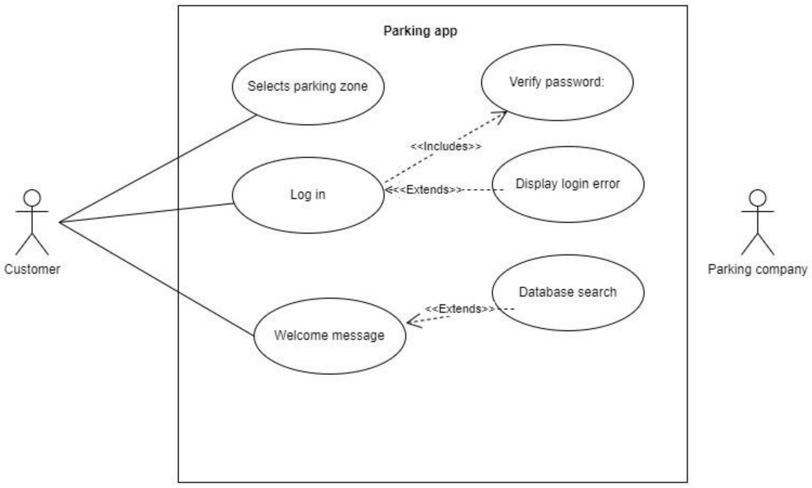


Figure 4. Use case diagram of a parking mobile application

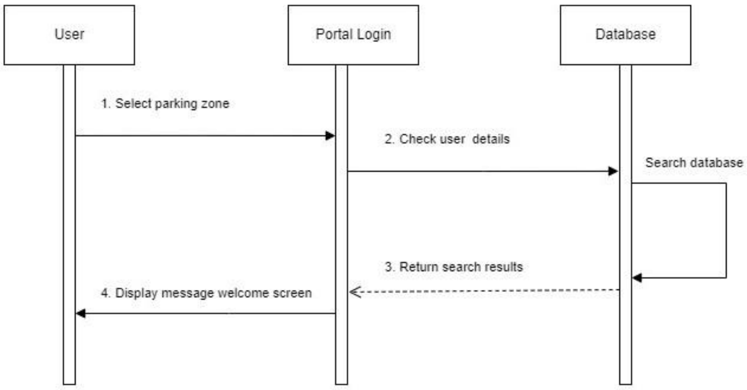


Figure 5. Sequence diagram of customer using a parking app

Findings

This section uses an attack tree, STRIDE, and UML diagrams to analysis real-world threats to Queens medical centre's ASMIS. Using an attack tree as a guide (see Figure 6), the STRIDE method can further analyse these actions.

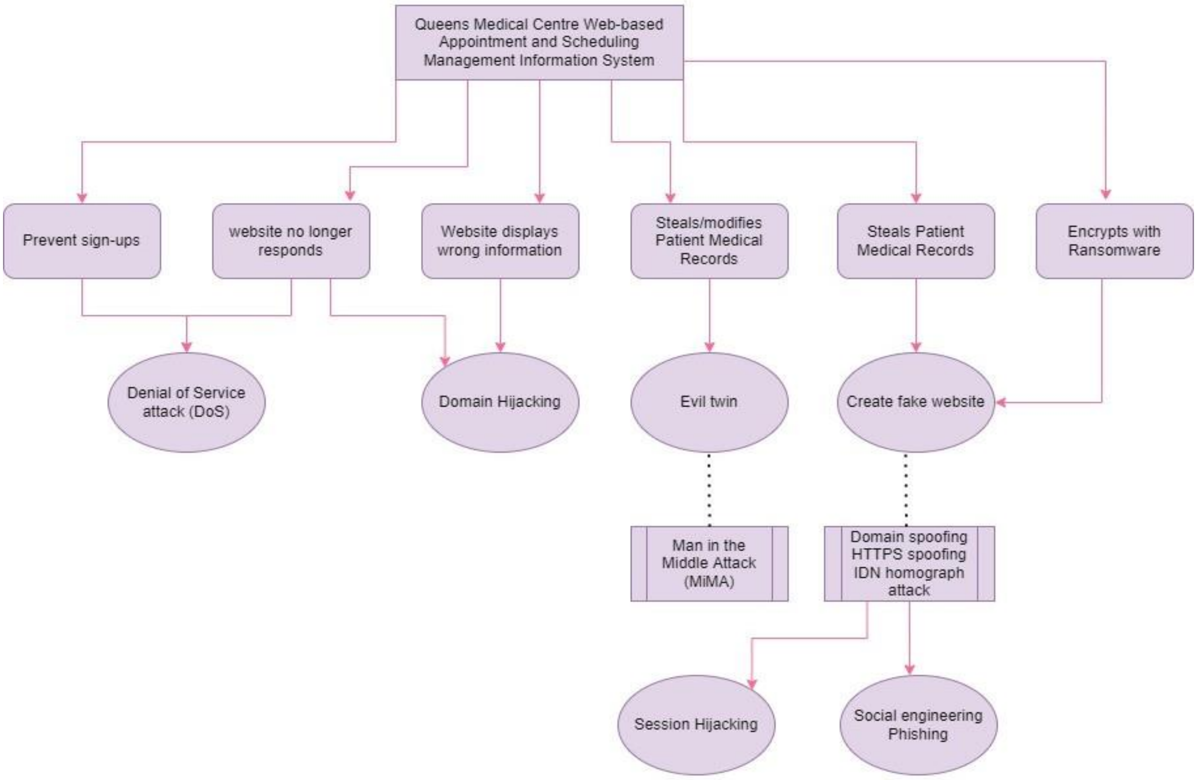

Queens Medical Centre Web-based Appointment and Scheduling Management Information System
Prevent sign-ups
website no longer responds
Website displays wrong information
Steals/modifies Patient Medical Records
Steals Patient Medical Records
Encrypts with Ransomware
Denial of Service attack (DoS)
Domain Hijacking
Evil twin
Create fake website
Man in the Middle Attack (MiMA)
Domain spoofing HTTPS spoofing IDN homograph attack
Session Hijacking
Social engineering Phishing

Figure 6. Attack Tree

Spoofing

Threat actors use session hijacking, social engineering HTTPS spoofing, and IDN homograph attacks to create a fake ASMIS landing page with a login portal where unsuspecting users input their credentials. It is then possible to a gather authentication credentials such as username and password to then enter ASMIS under the guise of a staff member or patient. This also includes downloading malicious email files infected with ransomware or using an evil twin router to mimic original Wi-Fi SSID.

Tampering

Once the attacker has authentication credentials, they can modify, delete, and steal patients and medical staff records on ASMIS database causing a loss of integrity. Furthermore, an attacker uses tampering to hide or delete traces of their presence by removing or overwriting log files which affects non-repudiation.

Repudiation

If the attacker uses stolen credentials to modify or delete patient records, then these actions will be logged with the staff member's information. Also, threat actors repudiate through IP and MAC spoofing, tracker-free emails, VPN proxy servers, and anonymous payment services such as Bitcoin. These repudiation techniques allow the attacker to deny performing such actions.

Information disclosure

Threat actors can access ASMIS database, staff emails, and file systems and publish on third party websites for financial gain. There is a higher probability this will happen if the stolen staff credentials have elevated privilege levels which can access sensitive parts of ASMIS.

Denial of service

Threat actors use Denial of Service attacks and domain hijacking to prevent patients using the web portal for appointments. There are two common types of DoS: Smurf attack and SYN flood. These type of flood attacks aim to saturate the host server with an overwhelming number of packets and handshakes causing the server to crash or shutdown (www.cisa.gov, 2009).

Elevation of Privilege

Threat actors use stolen credentials with different levels of authorisation to execute actions. For example, using the medical centre manager’s credentials to delete patient’s medical history from database. This type of spoofing greatly impacts non-repudiation as it allows the attacker to access and tamper parts of the system under the guise of a legitimate user.

The sequence diagram in Figure 7 demonstrates the timeline and flow of a patient logging in and accessing appointments for specialists and dates. If a threat actor were to gain patient's login in credentials, they would be authenticated and authorised to tamper (e.g., modify, delete) with the account and create bogus appointments with different medical specialists. This would deny the treatment to the patient and cause wastage of human and administrative resources.

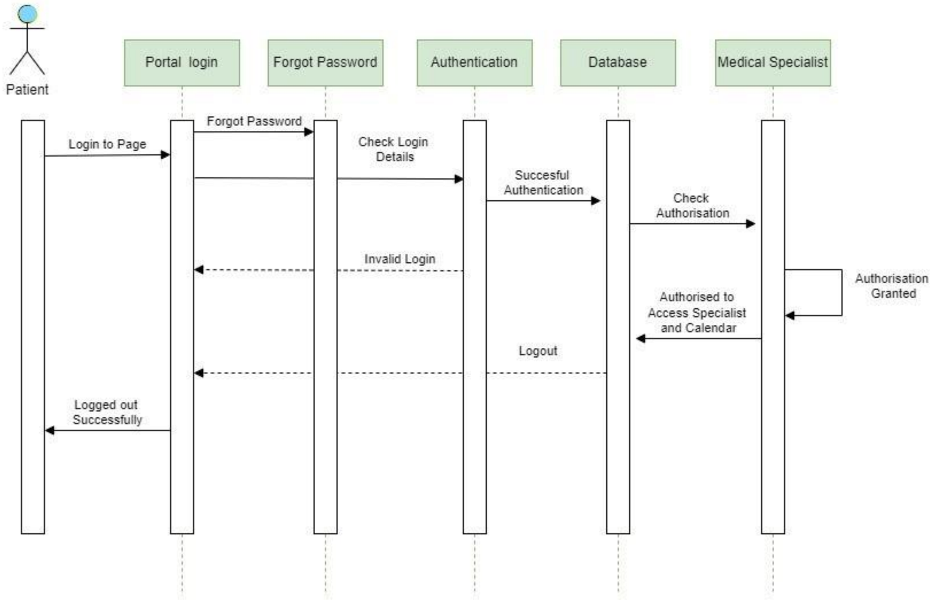


Figure 7. Sequence diagram of ASMIS log in portal

The use case diagram in Figure 8 clarifies and organises how patients and medical centre staff interact with ASMIS. Similar to Figure 8, threat actors can access the ASMIS through the administration portal with receptionist's credentials. Here, they can tamper with the appointment availability function and monitor the specialist's appointment and related patient information. Another scenario would be to change passwords to deny access for the receptionists and specialists.

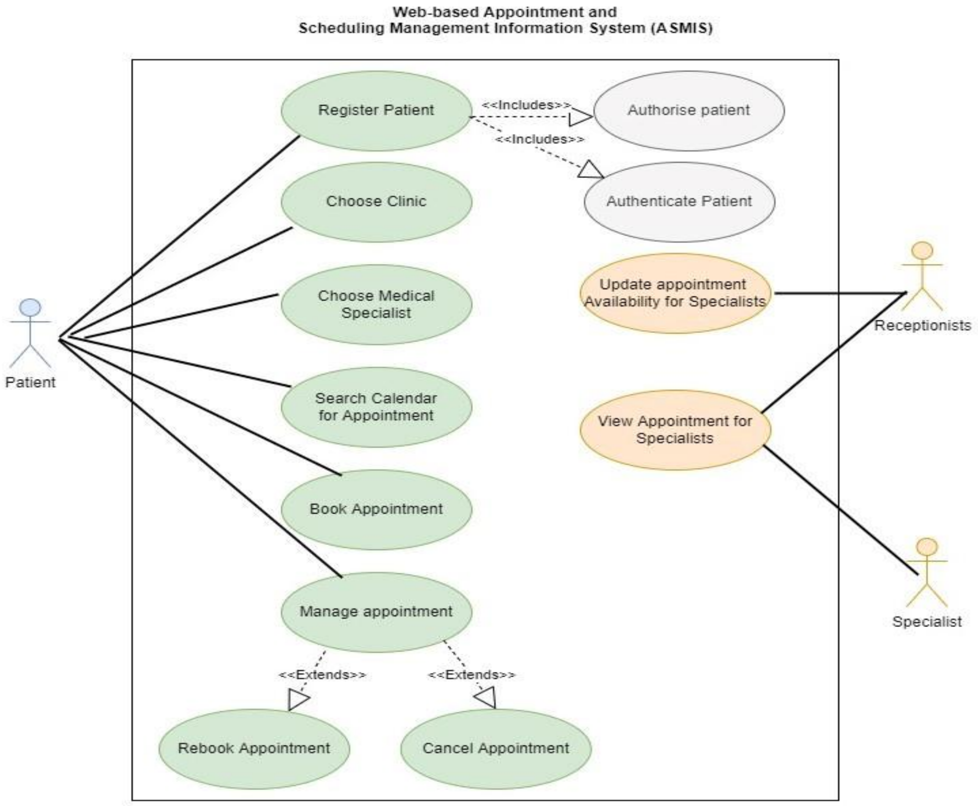


Figure 8. Use case Diagram of ASMIS

The class diagram in Figure 9 shows a four objects of a relational data model of ASMIS. If a threat actor gained credentials with elevated privilege, they could access the main ASMIS database and steal, delete or modify all user's data. Other threats include encrypting with ransomware. These type of database attacks are the most destructive as they cause near complete breakdown of the clinic's administrative, financial, care services.

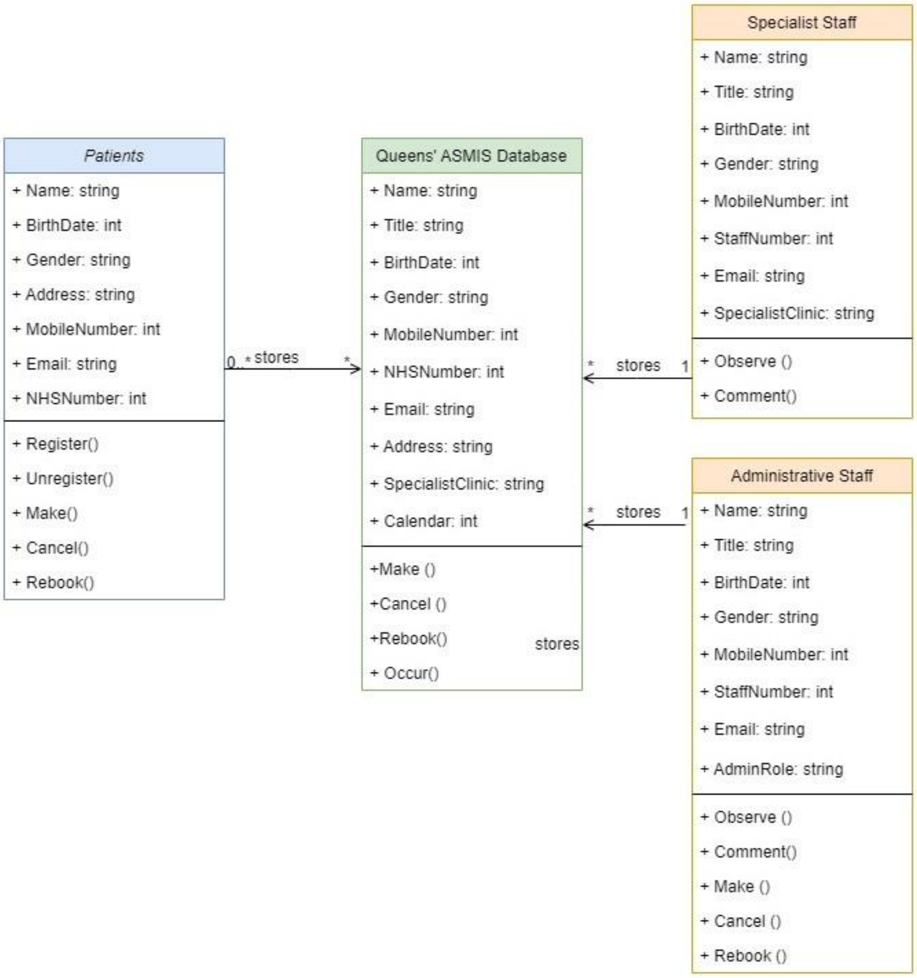


Figure 9. Class diagram of ASMIS database objects

Solutions

There are solutions to mitigate attacks on the ASMIS. Figure 10 illustrates defence strategies that encompass technical and human elements: awareness, training, and technology.

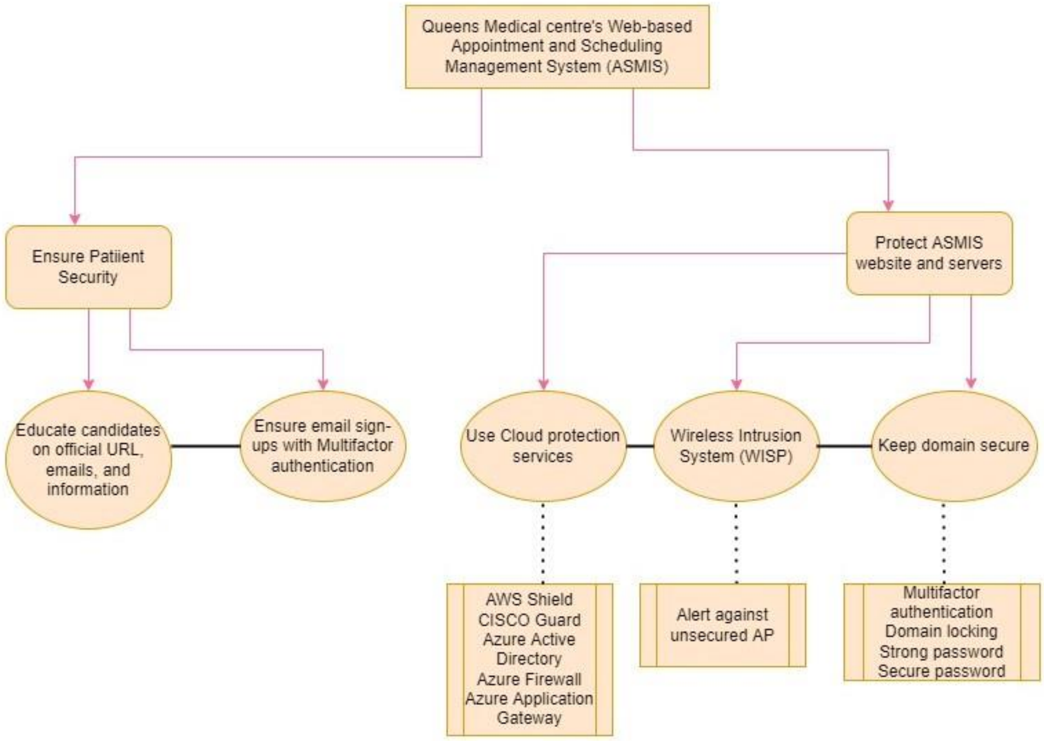

Queens Medical centre's Web-based Appointment and Scheduling Management System (ASMIS)
Ensure Patiient Security
Protect ASMIS website and servers
Educate candidates on official URL, emails, and information
Ensure email sign-ups with Multifactor authentication
Use Cloud protection services
Wireless Intrusion System (WISP)
Keep domain secure
AWS Shield
CISCO Guard
Azure Active Directory
Azure Firewall
Azure Application Gateway
Alert against unsecured AP
Multifactor authentication
Domain locking
Strong password
Secure password

Figure 10. Defence tree for ASMIS

Awareness

The National Cyber Security Council advises organisations to make aware of phishing-related threats. This can be done through in-house posters situated in the waiting room, patient leaflets, email, and face to face communication. These details include identifying phishing emails and what to do if victim of phishing (National Cyber Security Centre, 2019).

Training

Train all staff members in identifying and reporting all types of phishing. This is more crucial for members of staff who have elevated levels of privilege such as managers and database administrators who can be targeted by spear and whale fishing. Training can include, posters, simulations; quizzes, and infographics (National Cyber Security Centre, 2019). Other forms of training include identification and authentication prevention such as improving password complexity, changing default credentials and implementing log access controls and administration alerts (owasp.org, 2021).

Technology

Third party cloud service providers have a variety of functions and features which are built in or paid via subscription. Microsoft Active Directory and External Directory provides identity management for staff and customers with multifactor authentication and password management. To secure information and databases, Azure provides Sentinel and Information protection; and Application Gateway and Defender to protect against Denial of Service and secure web front ends (Microsoft, 2019).

Conclusion

This report has presented a multi-level approach to threat-driven modelling for ASMIS. It seems the most probable and destructive threats originate from social engineering attacks such as phishing and fake websites. With authorisation and authentication credentials, threat actors can cause disruption ranging from cancelling appointments to deleting the ASMIS database.

Yet, the easiest way reduce phishing is educate and train all users in identifying fraudulent emails and fake login pages as well as any suspicious behaviour. Cloud providers offer a multitude of services to protect the clinic's ASMIS namely Multifactor authentication, strong password management, and admin controls which can greatly increase ASMIS protection. However, there are caveats including training staff to monitor and administer services and developing effective cyber security-related policies and procedures.

References

Akinode, J. and Lekan (2007) Design and Implementation of a Patient Appointment and Scheduling System. International Advanced Research Journal in Science, Engineering and Technology ISO. Available from: https://www.researchgate.net/profile/Akinode-John-Lekan/publication/332864696_Design_and_Implementation_of_a_Patient_Appointment_and_Scheduling_System/links/5ccdf7c2a6fdccc9dd8d4628/Design-and-Implementation-of-a-Patient-Appointment-and-Scheduling-System.pdf [Accessed 20 Jan. 2022].

GOV.UK (2018) Data Protection. Available from: https://www.gov.uk/data-protection [Accessed 30 January 2022].

Ingoldsby, T. (2021) Attack Tree-based Threat Risk Analysis. Available from: https://www.amenaza.com/downloads/docs/AttackTreeThreatRiskAnalysis.pdf [Accessed 21 January 2022].

Khan, R., McLaughlin, K., Laverty, D. and Sezer, S. (2017) STRIDE-based threat modeling for cyber-physical systems. IEEE Xplore. Available from: https://ieeexplore.ieee.org/document/8260283 [Accessed 18 January 2022].

Kong, J. and Xu, D. (2008) A UML-Based Framework for Design and Analysis of Dependable Software. 2008 32nd Annual IEEE International Computer Software and Applications Conference. Available from: https://0-ieeexplore-ieee-org.serlib0.essex.ac.uk/document/4591528 [Accessed 9 January 2022].

Landi, H. (2017) Hack of Appointment System at Emory Healthcare Affects 80,000 Patient Records. Available from: https://www.hcinnovationgroup.com/cybersecurity/news/13028204/hack-of-appointment-system-at-emory-healthcare-affects-80000-patient-records [Accessed 20 January 2022].

Löhner, B. and Niedermayer, H. (2018) Attack-Defense-Trees and other Security Modeling Tools. Available from: https://www.semanticscholar.org/paper/Attack-Defense-Trees-and-other-Security-Modeling-L%C3%B6hner-Niedermayer/3809f354a97c3c67035ec1f8d4c555ba5c5659dd [Accessed 24 January 2022].

Microsoft (2019) Microsoft Azure Cloud Computing Platform & Services. Available from: https://azure.microsoft.com/en-us/ [Accessed 27 January 2022].

National Cyber Security Centre (2019) Phishing attacks: defending your organisation. Available at: https://www.ncsc.gov.uk/guidance/phishing [Accessed 27 January 2022].

Owasp.org. (2021) A07 Identification and Authentication Failures - OWASP Top 10:2021. Available from: https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/ [Accessed 27 January 2022].

Powerapps.microsoft.com. (2022) Portals – Low-Code App Portals | Microsoft Power Apps. Available from: https://powerapps.microsoft.com/en-us/portals/ [Accessed 19 January 2022].

Priestley, M. (2004) Practical object-oriented design with UML. Mcgraw-Hill.

PrivacyTrust (2018) GDPR. Available from: https://www.gdpr.org/ [Accessed 30 January 2022].

Rumbaugh, J., Booch, G. and Ivar Jacobson (2010) The unified modeling language reference manual. Boston: Addison-Wesley.

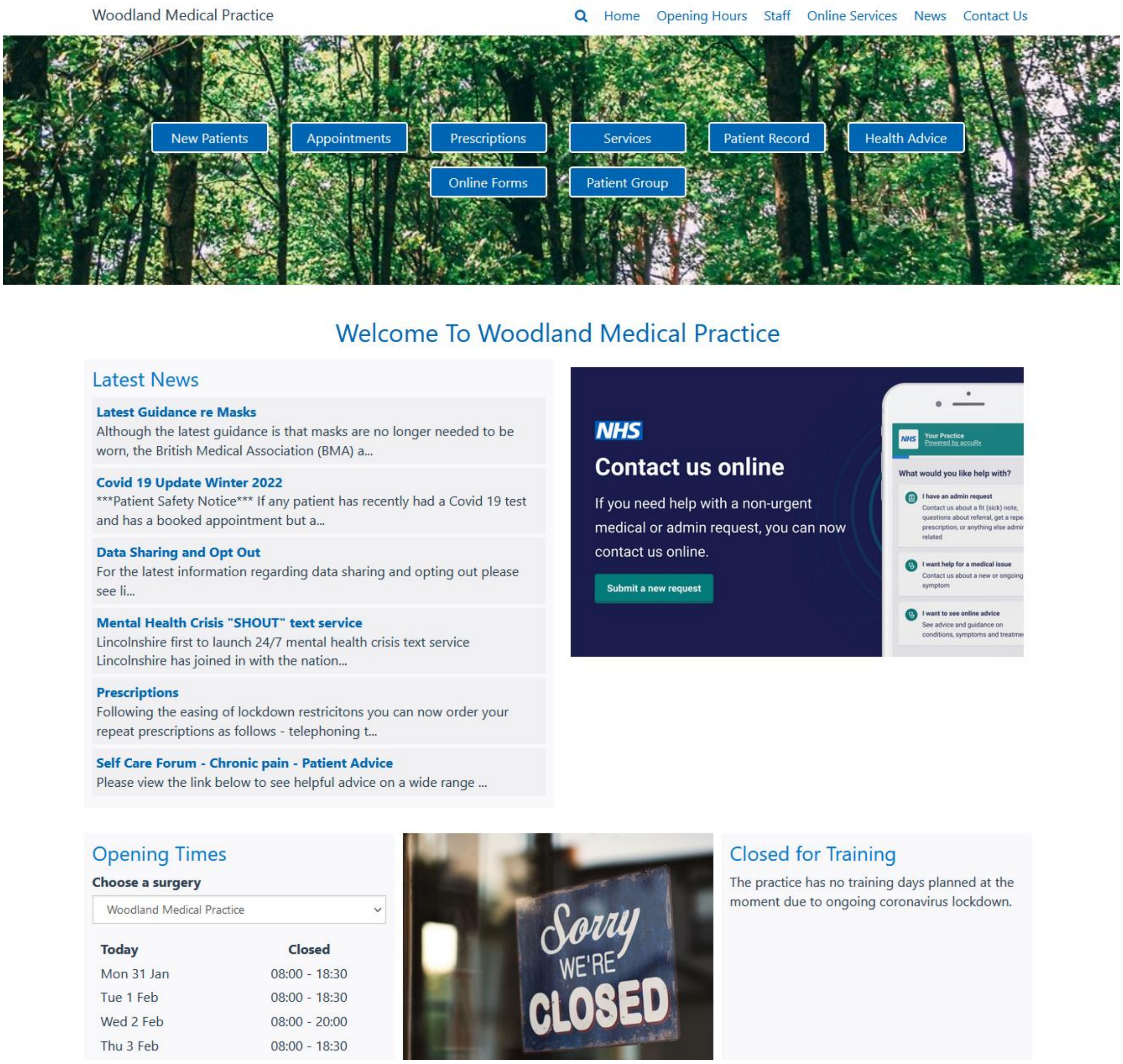
System Bookings. (2019) NHS. Available from: https://www.systembookings.com/clients/nhs-booking-system/ [Accessed 19 January 2022].

Woodlandmedicalpractice.org.uk. (2022) Woodland Medical Practice. Available from: https://www.woodlandmedicalpractice.org.uk/our-staff [Accessed 19 January 2022].

Zhao, P., Yoo, I., Lavoie, J., Lavoie, B.J. and Simoes, E. (2017) Web-Based Medical Appointment Systems: A Systematic Review. Journal of Medical Internet Research,19(4), p.e134. Available from: https://eds.p.ebscohost.com/eds/detail/detail?vid=0&sid=0a72ccab-6946-469c-abb7-00c2e6258a69%40redis&bdata=JnNpdGU9ZWRzLWxpdmU%3d#AN=28446422&db=mnh [Accessed 18 January 2022].

Appendix

Appendix A



Welcome To Woodland Medical Practice

Latest News

Latest Guidance re Masks
Although the latest guidance is that masks are no longer needed to be worn, the British Medical Association (BMA) a...

Covid 19 Update Winter 2022
Patient Safety Notice If any patient has recently had a Covid 19 test and has a booked appointment but a...

Data Sharing and Opt Out
For the latest information regarding data sharing and opting out please see li...

Mental Health Crisis "SHOUT" text service
Lincolnshire first to launch 24/7 mental health crisis text service Lincolnshire has joined in with the nation...

Prescriptions
Following the easing of lockdown restricitons you can now order your repeat prescriptions as follows - telephoning t...

Self Care Forum - Chronic pain - Patient Advice
Please view the link below to see helpful advice on a wide range ...

Contact us online

If you need help with a non-urgent medical or admin request, you can now contact us online.

What would you like help with?

I have an admin request
Contact us about a fit (sick) note, questions about referral, get a repe prescription, or anything else admir related

I want help for a medical issue
Contact us about a new or ongoing symptom

I want to see online advice
See advice and guidance on conditions, symptoms and treatme

Opening Times

Choose a surgery

Woodland Medical Practice

Today	**Closed**
Mon 31 Jan	08:00 - 18:30
Tue 1 Feb	08:00 - 18:30
Wed 2 Feb	08:00 - 20:00
Thu 3 Feb	08:00 - 18:30

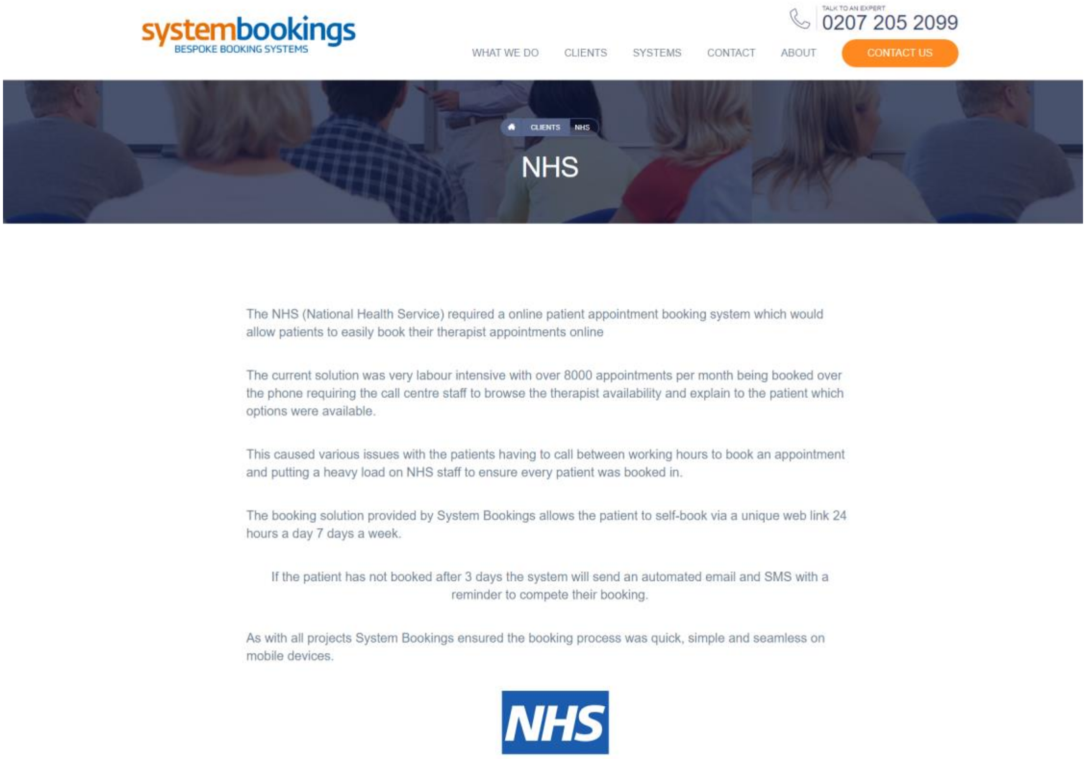
Closed for Training

The practice has no training days planned at the moment due to ongoing coronavirus lockdown.

Source: woodlandmedicalpractice.org.uk (2022)

Appendix B

System Bookings’ Cloud-based ASMIS



NHS

The NHS (National Health Service) required a online patient appointment booking system which would allow patients to easily book their therapist appointments online

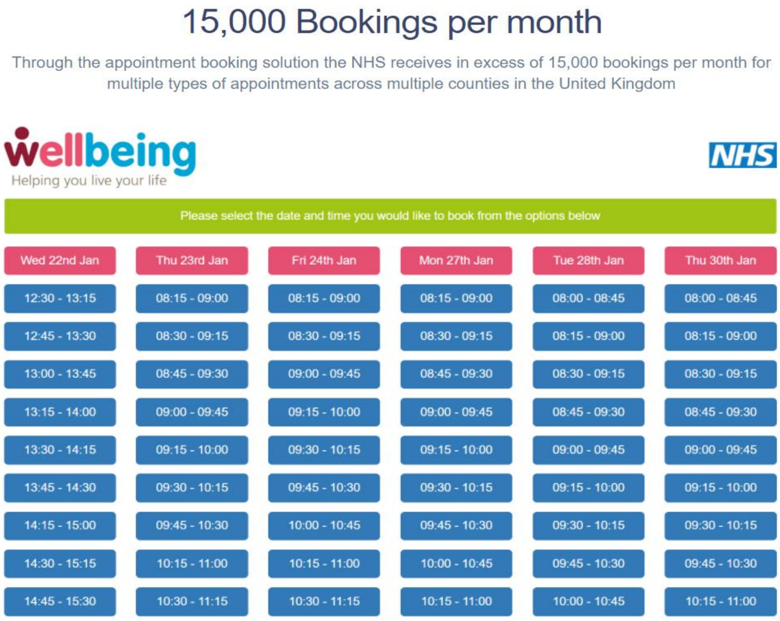
The current solution was very labour intensive with over 8000 appointments per month being booked over the phone requiring the call centre staff to browse the therapist availability and explain to the patient which options were available.

This caused various issues with the patients having to call between working hours to book an appointment and putting a heavy load on NHS staff to ensure every patient was booked in.

The booking solution provided by System Bookings allows the patient to self-book via a unique web link 24 hours a day 7 days a week.

If the patient has not booked after 3 days the system will send an automated email and SMS with a reminder to compete their booking.

As with all projects System Bookings ensured the booking process was quick, simple and seamless on mobile devices.



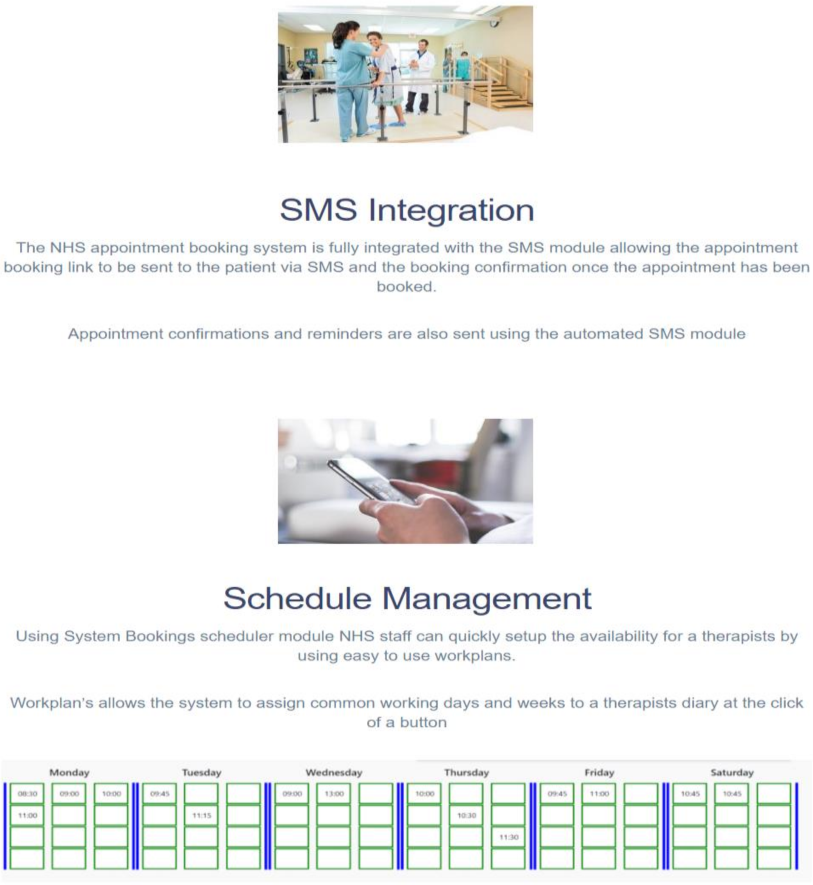
15,000 Bookings per month

Through the appointment booking solution the NHS receives in excess of 15,000 bookings per month for multiple types of appointments across multiple counties in the United Kingdom

Please select the date and time you would like to book from the options below

Wed 22nd Jan	Thu 23rd Jan	Fri 24th Jan	Mon 27th Jan	Tue 28th Jan	Thu 30th Jan
12:30 - 13:15	08:15 - 09:00	08:15 - 09:00	08:15 - 09:00	08:00 - 08:45	08:00 - 08:45
12:45 - 13:30	08:30 - 09:15	08:30 - 09:15	08:30 - 09:15	08:15 - 09:00	08:15 - 09:00
13:00 - 13:45	08:45 - 09:30	09:00 - 09:45	08:45 - 09:30	08:30 - 09:15	08:30 - 09:15
13:15 - 14:00	09:00 - 09:45	09:15 - 10:00	09:00 - 09:45	08:45 - 09:30	08:45 - 09:30
13:30 - 14:15	09:15 - 10:00	09:30 - 10:15	09:15 - 10:00	09:00 - 09:45	09:00 - 09:45
13:45 - 14:30	09:30 - 10:15	09:45 - 10:30	09:30 - 10:15	09:15 - 10:00	09:15 - 10:00
14:15 - 15:00	09:45 - 10:30	10:00 - 10:45	09:45 - 10:30	09:30 - 10:15	09:30 - 10:15
14:30 - 15:15	10:15 - 11:00	10:15 - 11:00	10:00 - 10:45	09:45 - 10:30	09:45 - 10:30
14:45 - 15:30	10:30 - 11:15	10:30 - 11:15	10:15 - 11:00	10:00 - 10:45	10:15 - 11:00

Source: System Bookings (2019)



SMS Integration

The NHS appointment booking system is fully integrated with the SMS module allowing the appointment booking link to be sent to the patient via SMS and the booking confirmation once the appointment has been booked.

Appointment confirmations and reminders are also sent using the automated SMS module

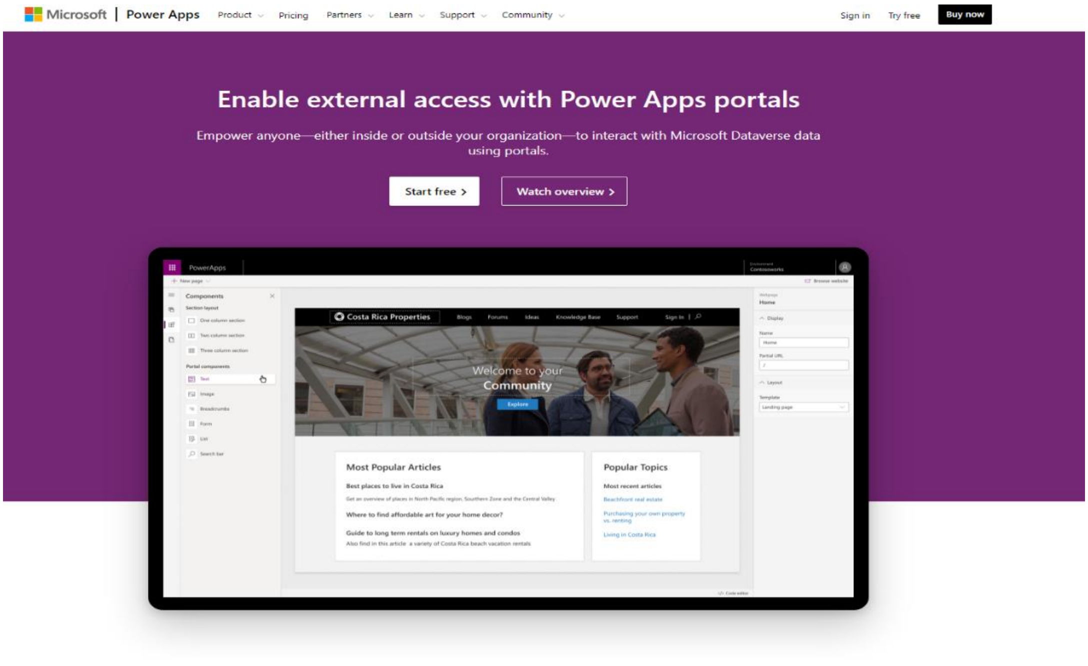
Schedule Management

Using System Bookings scheduler module NHS staff can quickly setup the availability for a therapists by using easy to use workplans.

Workplan's allows the system to assign common working days and weeks to a therapists diary at the click of a button

Monday			Tuesday			Wednesday			Thursday			Friday			Saturday		
08:30	09:00	10:00	09:45			09:00	13:00		10:00			09:45	11:00		10:45	10:45	
11:00				11:15						10:30							
											11:30						

Microsoft’s Power Apps cloud-based portal



Enable external access with Power Apps portals

Empower anyone—either inside or outside your organization—to interact with Microsoft Dataverse data using portals.

Welcome to your Community

Most Popular Articles

Best places to live in Costa Rica

Get an overview of places in North Pacific region, Southern Zone and the Central Valley

Where to find affordable art for your home decor?

Guide to long term rentals on luxury homes and condos

Also find in this article a variety of Costa Rica beach vacation rentals

Popular Topics

Most recent articles

Beachfront real estate

Purchasing your own property vs. renting

Living in Costa Rica

Source: Powerapps.microsoft.com (2022)